AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1. – 20. (Cancelled)

21. (Currently Amended) A method for managing security of at least one additional application associated to a main application with a security module of an equipment connected, via a network, to a control server managed by an operator, the main application and the additional applications use resources as data or functions stored in the security module locally connected to said equipment, ~~the method being carried out on at least one of each initialization, activation or deactivation of the at least one additional application~~, comprising:

- ~~receiving via the network, by the control server~~ the equipment, periodically sending via the network to the control server identification data including at least a type and software version of the equipment and ~~an identifier~~ a type and software version of the security module,
- analyzing and verifying by the control server the identification data upon an occurrence of at least one:

after each connection of the equipment to the network,

after each updating of the software version of the equipment,

after at least one of each activation and deactivation of the additional application on the equipment,

after each updating of the software version of the security module,

after each updating of resources on the security module, and

periodically at a rate given by the control server,

- generating, by the control server, a cryptogram from a result of the verification of the identification data by comparing the identification data to a subscriber database content,
- transmitting, by the control server, the cryptogram, via the network and the equipment, to the security module,
- receiving and analyzing the cryptogram by the security module for acting on specific applications according to instructions included in the cryptogram, and
- selectively activating or deactivating at least one resource as data or functions stored in said security module by executing the instructions included in the cryptogram and using the selected resource to condition the functioning of the at least one additional application stored in the equipment according to criteria established by at least one of a supplier of said additional application[[,]] or the operator managing the control server ~~and a user of the equipment~~,

wherein the resources as data or functions of the security module used by the main application are left active for connection of the equipment to the network so as to obtain further cryptograms from the control server.

22. (Previously Presented) The method according to claim 21, wherein the equipment is a mobile equipment of mobile telephony.

23. (Previously Presented) The method according to claim 21, wherein the network is a mobile network of the GSM, GPRS or UMTS type.

24. (Previously Presented) A method according to claim 21, wherein the security module is a subscriber module of a SIM card type inserted into a mobile equipment of mobile telephony.

25. (Previously Presented) The method according to claim 24, wherein the identification data of at least one of the mobile equipment and the subscriber module comprises an identifier of the mobile equipment and an identifier of the subscriber module pertaining to a subscriber to the mobile network.

26. (Previously Presented) The method according to claim 21, wherein the criteria defines usage limits of the additional application according to risks associated to the additional application and to the type and the software version of the equipment that at least one of the operator, the application supplier and the user of the-equipment take in account.

27. - 33. (Cancelled)

34. (Previously Presented) The method according to claim 25, wherein the subscriber module, prior to the execution of the instructions included in the cryptogram, compares the identifier of the mobile equipment with that previously

received and only initiates analyzing an verifying by the control server of the identification data if the identifier of the mobile equipment has changed.

35. (Previously Presented) The method according to claim 25, wherein the control server, prior to the transmission of the cryptogram, compares the identifier of the mobile equipment with that previously received and only initiates analyzing and verifying the identification data if the identifier of the mobile equipment has changed.

36. (Previously Presented) The method according to claim 25, wherein the cryptogram is made up of a message encrypted by the control server with the aid of an asymmetrical or symmetrical encryption key from a data set containing, among other data, the identifier of the mobile equipment, the identifier of the subscriber module, resource references of the subscriber module and a predictable variable.

37. (Previously Presented) The method according to claim 36, wherein the subscriber module transmits to the control server, via the mobile equipment and the mobile network, a confirmation message when the subscriber module has received the cryptogram, said message confirming correct reception and the adequate processing of the cryptogram by the subscriber module.

38. (Previously Presented) The method according to claim 21, wherein the equipment is a Pay-TV decoder or a computer to which the security module is connected.

39. (Currently Amended) A security module including resources as data or functions intended to be locally accessed by a main application and at least one additional application installed in an equipment connected, via a network, to a control server configured for managing security of the at least one additional application on at least one of each initialization, activation or deactivation of the at least one additional application, comprising:

a device for reading and transmitting identification data periodically via the network to the control server including at least ~~an identifier of~~ a type and software version of the equipment and ~~an identifier~~ a type and software version of the security module;

a device for analyzing and verifying the identification data upon an occurrence of at least one:

after each connection of the equipment to the network,

after each updating of the software version of the equipment,

after at least one of each activation and deactivation of the additional application on the equipment,

after each updating of the software version of the security module,

after each updating of resources on the security module, and

periodically at a rate given by the control server,

a device for generating a cryptogram from a result of the verification of the identification data by comparing the identification data to a subscriber database content;

a device for receiving and analyzing [[a]] the cryptogram ~~sent by the control server~~ for acting on specific applications according to instructions included in the cryptogram; and

a device for selectively activating or deactivating at least one resource as data or functions stored in the security module by executing the instructions included in the cryptogram and using the selected resource to condition the functioning of the at least one additional application stored in the equipment according to criteria established by at least one of the supplier of said additional application[[,]] or the operator managing the control server ~~and a user of the equipment~~,

wherein the resources as data or functions of the security module used by the main application are left active for connection of the equipment to the network so as to obtain further cryptograms from the control server.

40. (Previously Presented) The security module according to claim 39, constituting a subscriber module of a SIM card type connected to a mobile equipment.